

Attorney's Docket No. 83,820
Application No. 10/693,843
Page 3

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A central processing unit comprising:

means for processing computer instructions comprising means for receiving computer instructions and means for executing computer instructions;

a secure memory unit coupled to said processing means, said secure memory unit having one or more resident security check programs for identifying whether the computer has been tampered with;

~~wherein when~~ said means for processing information arranged to receive receives a secure attention instruction from a source through said receiving means and thereafter said means for executing computer instructions executes the security check program by retrieving its instructions from the secure memory,

wherein if a deceptive interpreter is not present, the means for processing information retrieves and executes the at least one security check program, evaluates the results of the security check program, and transmits the results of the security check program and a cryptographically generated authentication value to the source,

wherein if a deceptive interpreter is present, the computer processor will not retrieve and

Attorney's Docket No. 83,820
Application No. 10/693,843
Page 4

execute the security check program and will not transmit a correct authentication value to the source.

and wherein an incorrect or absent authentication value indicates the presence of a deceptive interpreter.

2. (Original) The central processing unit of claim 1 wherein said means for receiving computer instructions is a system bus.
3. (Original) The central processing unit of claim 1 wherein said means for executing computer instructions is at least one processor.
4. (Original) The central processing unit of claim 1 wherein access to said secure memory unit coupled to said processing means is restricted to the processing means in the absence of a cryptographically validated administrative secure attention instruction.
5. (Original) The central processing unit of claim 1 wherein said security check programs comprises a cryptographic check key, and upon the execution of the security check program if the result of the check program is satisfactory, the cryptographic check key is used to authenticate the result values transmitted to the source of the secure attention instruction.

Attorney's Docket No. 83,820

Application No. 10/693,843

Page 5

6. (Original) The central processing unit of claim 4 wherein said security check programs comprises a cryptographic check key, and upon the execution of the security check program if the result of the check program is satisfactory, the cryptographic check key is used to authenticate the result values transmitted to the source of the secure attention instruction.
7. (Original) The central processing unit of claim 4 wherein the secure attention instruction is issued by an external source and received by the CPU through a first program.
8. (Original) The central processing unit of claim 7 wherein the secure attention instruction is issued by a mobile software agent that executes on a secure computer system.
9. (Original) The central processing unit of claim 6 wherein the secure attention instruction is issued by an external source and received by the CPU through the first program.
10. (Original) The central processing unit of claim 9 wherein the secure attention instruction is issued by a mobile software agent that executes on a secure computer system.
11. (Currently Amended) A secure computer system comprising:
a central processing unit (CPU) for executing conventional instructions and secure attention instructions;

Attorney's Docket No. 83,820
Application No. 10/693,843
Page 6

a secure memory unit coupled to the CPU, the secure memory unit containing one or more check programs therein, the memory unit is configured to limit access to the check programs to only the CPU in the absence of a cryptographic key;

a computer readable medium coupled to the CPU through a first program,
a second program contained on the computer readable medium accessed by the CPU through said first program;

wherein upon the receipt of a secure attention instruction by the CPU, ~~the CPU, and executes one or more check programs from the secure memory unit for determining whether the computer has been tampered with; upon completion of the check programs, the CPU returns results of the check programs authenticated with a cryptographic value~~

if a deceptive interpreter is not present, the CPU retrieves and executes the at least one security check program, evaluates the results of the security check program, and transmits the results of the security check program and a cryptographically generated authentication value to the source, and

if a deceptive interpreter is present, the computer processor will not retrieve and execute the security check program and will not transmit a correct authentication value to the source, and wherein an incorrect or absent authentication value indicates the presence of a deceptive interpreter.

Attorney's Docket No. 83,820

Application No. 10/693,843

Page 7

12. (Original) The secure computer system of claim 11 wherein the first program is the operating system alternatively the secure memory unit is accessible via an external connection that bypasses the CPU and all other parts of the secure computer system for the purposes of managing the check programs.

13. (Original) The secure computer system of claim 12 wherein the secure attention instruction is issued by an external source and received by the CPU through the first program.

14. (Original) The secure computer system of claim 13 wherein the secure attention instruction is issued by a mobile software agent that executes on a secure computer system.

15. (Original) The secure computer system of claim 11 wherein the computer readable medium is a memory storage unit.

16. (Original) The secure computer system of claim 15 wherein the second program contains executable code.

17. (Original) The secure computer system of claim 11 wherein the secure memory unit is accessible via an external connection that bypasses the CPU and all other parts of the secure computer system upon the completion of a cryptographic authentication protocol.

Attorney's Docket No. 83,820

Application No. 10/693,843

Page 8

18. (Currently Amended) A central processing unit comprising:

means for processing computer instructions comprising means for receiving computer instructions and means for executing computer instructions;

a secure memory unit coupled to said processing means, said secure memory unit having one or more resident security check programs therein;

wherein ~~when~~ said means for processing information is arranged to receive receives a secure attention instruction through said receiving means from a source, said means for executing computer instructions is adapted to execute ~~executes~~ the security check program by retrieving its instructions from the secure memory, the security check program determining whether the computer has been tampered with;

wherein if a deceptive interpreter is not present, the processing means retrieves and executes the at least one security check program, evaluates the results of the security check program, and transmits the results of the security check program and a cryptographically generated authentication value to the source,

wherein if a deceptive interpreter is present, the processing means will not retrieve and execute the security check program and will not transmit a correct authentication value to the source,

and wherein an incorrect or absent authentication value indicates the presence of a deceptive interpreter

Attorney's Docket No. 83,820

Application No. 10/693,843

Page 9

~~wherein said security check programs comprise a cryptographic check key, and upon the execution of the security check program if the result of the check program is satisfactory, the cryptographic check key is used to authenticate the result values transmitted to the source of the secure attention instruction.~~

19. (Canceled)

20. (Previously presented) The system according to claim 1, wherein the security check programs determine whether at least one of malicious instructions, viruses, deceptive interpreters, and Trojan horses is present.

21.-22 (Canceled)

23. (Currently Amended) A method for ~~checking the security of a computer system~~
determining whether a computer has been tampered with by a deceptive interpreter, comprising:

a computer processor receiving a secure attention instruction from a source external to the processor and transferring the secure attention instruction to a secure memory unit coupled to the computer processor, the secure memory unit having at least one security check program,

wherein if a deceptive interpreter is not present, the computer processor retrieves and executes the at least one security check program, evaluates the results of the security check

Attorney's Docket No. 83,820
Application No. 10/693,843
Page 10

program, and transmits the results of the security check program and a cryptographically generated authentication value to the source,

wherein if a deceptive interpreter is present, the computer processor will not retrieve and execute the security check program and will not transmit a correct authentication value to the source,

and wherein an incorrect or absent authentication value indicates the presence of a deceptive interpreter

~~retrieving and executing at least one security check program from the secure memory unit, the security check program determining whether the computer has been tampered with, and transmitting results of the security check program and an authentication value from the secure memory unit to the source.~~

24.-25. (Canceled)

26. (Previously presented) The method according to claim 23, further comprising:
the source transmitting the secure attention instruction to the computer processor.

27. (Previously presented) The method according to claim 23, wherein the source is an autonomous mobile software agent.

Attorney's Docket No. 83,820

Application No. 10/693,843

Page 11

28. (Previously presented) The method according to claim 23, further comprising:
the computer processor interrupting execution of other instructions after receipt of the
secure attention instruction.

29.-31. (Canceled)